SSA-604937: Multiple Web Server Vulnerabilities in Opcenter Execution Core

Publication Date: 2020-07-14
Last Update: 2021-01-12
Current Version: V1.2
CVSS v3.1 Base Score: 8.5

SUMMARY

Opcenter Execution Core (formerly known as Camstar Enterprise Platform) contains a cross-site scripting (CVE-2020-7576), an SQL injection (CVE-2020-7577), a privilege escalation (CVE-2020-7578), and an information disclosure vulnerability (CVE-2020-28930) in various versions of the product.

Siemens has released an update for Opcenter Execution Core and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Camstar Enterprise Platform: All versions only affected by CVE-2020-7576, CVE-2020-7577, CVE-2020-7578	Update to Opcenter Execution Core V8.4 or later version https://support.sw.siemens.com/ (login required)
Opcenter Execution Core: All versions < V8.2 only affected by CVE-2020-7576, CVE-2020-7577, CVE-2020-7578	Update to Opcenter Execution Core V8.4 or later version https://support.sw.siemens.com/ (login required)
Opcenter Execution Core: V8.2 only affected by CVE-2020-7576, CVE-2020-28390	Update to Opcenter Execution Core V8.4 or later version https://support.sw.siemens.com/ (login required)
Opcenter Execution Core: V8.3 only affected by CVE-2020-28390	Update to Opcenter Execution Core V8.4 or later version https://support.sw.siemens.com/ (login required)

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Configure a web application firewall to filter traffic containing XSS Injection and SQL Injections
- Restrict access to application webserver for trusted users only
- CVE-2020-7576: Review access permissions for the application and limit the number of users with the ability to create containers, packages, or to register defects
- CVE-2020-28390: Ensure that only trusted persons have access to Opcenter Execution Core servers

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals.

Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

Opcenter Execution Core (formerly known as Camstar Enterprise Platform) by Siemens PLM Software is a universal usable Manufaturing Execution System (MES). This product allows manufacturers to significantly increase the quality of a product during manufacturing process. The process begins with the planning, supply management, quality management, stretching to production and even to customer service. This effectively supports the whole product life-cycle.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2020-7576

An authenticated user with the ability to create containers, packages or register defects could perform stored Cross-Site Scripting (XSS) attacks within the vulnerable software.

The impact of this attack could result in the session cookies of legitimate users being stolen. Should the attacker gain access to these cookies, they could then hijack the session and perform arbitrary actions in the name of the victim.

CVSS v3.1 Base Score	8.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Vulnerability CVE-2020-7577

Through the use of several vulnerable fields of the application, an authenticated user could perform an SQL Injection attack by passing a modified SQL query downstream to the back-end server.

The exploit of this vulnerability could be used to read, and potentially modify application data to which the user has access to.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2020-7578

Authenticated users could have access to resources they normally would not have. This vulnerability could allow an attacker to view internal information and perform unauthorized changes.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-284: Improper Access Control

Vulnerability CVE-2020-28390

The application contains an information leakage vulnerability in the handling of web client sessions.

A local attacker who has access to the Web Client Session Storage could disclose the passwords of currently logged-in users.

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-522: Insufficiently Protected Credentials

ADDITIONAL INFORMATION

These vulnerabilities have been discovered internally by Siemens.

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2020-07-14):	Publication Date
V1.1 (2020-08-11):	Errata: CVE-2020-7576 was not yet fixed in Opcenter Execution Core V8.2
V1.2 (2021-01-12):	Added additional vulnerability CVE-2020-28390 and latest releases of Opcenter Exceution Core (V8.3, V8.4)

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.